UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,509	12/19/2001	Richard E. Kessler	005655.P004	6406

8791 7590 03/02/2006

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/025,509	KESSLER ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 26, 2006 has been entered.

2. Claims 1-34 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-34 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejetions - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-15 and 25-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blaker (hereinafter Blaker) United States Publication Number 2002/0004904 in view of Bellwood (hereinafter Bellwood) United States Letter Patent Number 6,584,567 and in view of Mauro et al. (hereinafter Mauro) Unites States Publication Number 2002/0146128.

As per claims 1 and 25:

Blaker teaches a computer implemented method comprising:

calling with an instruction operation from a first processor; (Page 2, paragraph 11; one or more operands are downloaded ...from the system memory)

executing a plurality of primitive security operations at a second processor in response to receiving the instruction operation from the first processor; (Page 2, paragraph 11)

generating a set of data from executing the plurality of primitive security operations; (Page 2, paragraph 11) and

Blaker does not explicitly disclose calling with a single macro instruction operation, the single macro instruction operation representing a plurality of primitive security operations; and establishing a secure session with the set of data.

Mauro in analogous art, however, discloses calling with a single macro instruction operation, the single macro instruction operation representing a plurality of primitive security operations; (Page 2, paragraphs 27-28; Page 3, paragraph 29; when a primitive cryptographic function is required, the CPU downloads the DSP assembly

image, downloadable executable instructions executed by the DSP, through the shared memory)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker to include calling with a single macro instruction operation, the single macro instruction operation representing a plurality of primitive security operations. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to accelerate the performance of complex encryption and authentication algorithms needed in implementing security protocols, such as SSL, IPSec and WAP with a minimum delay and a minimum cost. (Page 1, paragraphs 5-6, Mauro)

Both references do not explicitly disclose establishing a secure session with the set of data. Bellwood in analogous art, however, discloses a method of establishing a secure session between client browser and a server. (Col. 2, lines 19-22).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker and Mauro to include a method of establishing a secure session with the set of data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Bellwood (Col. 1, lines 56-58) in order to provide a mechanism that reduces network resource demands and enhancing secure communication between devices.

As per claims 2, 12 and 26:

The combination of Blaker, Mauro and Bellwood teaches all the subject matter as discussed above. In addition, Blaker further discloses a computer implemented method wherein the set of data comprises: a set of decrypted data; (Page 6, paragraph 54) a set of encrypted data; (Page 6, paragraph 54) and a set of hashed messages. (Page 6, paragraph 54)

As per claims 3 and 27:

The combination of Blaker, Mauro and Bellwood teaches all the subject matter as discussed above. In addition, Blaker further discloses a computer implemented method comprising a set of random numbers. (Page 4, paragraph 34)

As per claims 4 and 28:

The combination of Blaker, Mauro and Bellwood teaches all the subject matter as discussed above. In addition, Bellwood further discloses a computer implemented method comprising the first processor calling a second operation to establish a second secure session. (Col. 2, lines 49-50)

As per claims 5 and 29:

The combination of Blaker, Mauro and Bellwood teaches all the subject matter as discussed above. In addition, Mauro further discloses a computer implemented method wherein the secure session is an SSL 3.0 session, a TLS session, or an IPSec session. (Page 2, paragraph 20)

As per claims 6 and 30:

Blaker teaches a computer implemented method comprising:

calling with an instruction operation from a first processor; (Page 2, paragraph 11; one or more operands are downloaded ...from the system memory)

executing a plurality of primitive security operations at a second processor in response to receiving the instruction operation from the first processor; (Page 2, paragraph 11)

generating a set of data from executing the plurality of primitive security operations; (Page 2, paragraph 11) and

Blaker does not explicitly disclose calling with a single macro instruction operation, the single macro instruction operation representing a plurality of primitive security operations; set of operations comprising: generating a secret and a key material, creating a first finished hash for a client message, creating a second finished hash for a server message, creating a finished message; and establishing a secure session.

Mauro in analogous art, however, discloses calling with a single macro instruction operation, the single macro instruction operation representing a plurality of primitive security operations; (Page 2, paragraphs 27-28; Page 3, paragraph 29; when a primitive cryptographic function is required, the CPU downloads the DSP assembly image, downloadable executable instructions executed by the DSP, through the shared memory)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker to include calling with a single macro instruction operation, the single macro instruction operation

representing a plurality of primitive security operations. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to accelerate the performance of complex encryption and authentication algorithms needed in implementing security protocols, such as SSL, IPSec and WAP with a minimum delay and a minimum cost. (Page 1, paragraphs 5-6, Mauro)

Both references do not explicitly disclose set of operations comprising: generating a secret and a key material, creating a first finished hash for a client message, creating a second finished hash for a server message, creating a finished message; and establishing a secure session.

Bellwood in analogous art, however, disclose a method of generating a secret and a key material, (Col. 9, lines 2-5) creating a first finished hash for a client message, (Figures 3A and 3B; Col. 9, lines 6-10) creating a second finished hash for a server message, (Figures 3A and 3B; Col. 9, lines 6-10) creating a finished message; (Figures 3A and 3B) and establishing a secure session. (Col. 2, lines 19-22).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker and Mauro to include set of operations comprising: generating a secret and a key material, creating a first finished hash for a client message, creating a second finished hash for a server message, creating a finished message; and establishing a secure session. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Bellwood (Col. 1, lines 56-58) in

order to provide a mechanism that reduces network resource demands and enhancing secure communication between devices.

As per claims 7 and 31:

The combination of Blaker, Mauro and Bellwood teaches all the subject matter as discussed above. In addition, Bellwood further discloses a computer implemented method wherein the set of operations further comprises decrypting a pre-master secret; and decrypting a client finished message. (Col. 9, lines 1-5)

As per claims 8 and 32:

The combination of Blaker, Mauro and Bellwood teaches all the subject matter as discussed above. In addition, Blaker further discloses a computer implemented method wherein the set of operations further comprises generating a set of random numbers. (Page 4, paragraph 34)

As per claims 9 and 33:

The combination of Blaker, Mauro and Bellwood teaches all the subject matter as discussed above. In addition, Bellwood further discloses a computer implemented method wherein the set of operations further comprises creating an expected finished message. (Figures 3A and 3B)

As per claims 10 and 34:

The combination of Blaker, Mauro and Bellwood teaches all the subject matter as discussed above. In addition, Bellwood further discloses a computer implemented method comprising calling a second macro security operation to establish a second secure session. (Col. 2, lines 49-50)

As per claim 11:

Bellwood teaches a system comprising:

a first network element to request a secure session; (Col. 5, lines 30-31, Bellwood) and

a second network element networked to the first network element, the second network element to call a macro security operation from a first processor, (Col. 5, lines 32-37, Bellwood)

Bellwood does not explicitly disclose a macro security operation associated with a plurality of primitive security operation; executing a plurality of primitive security operations at a second processor in response to the macro security operation, and to generate a set of data from the execution of the plurality of primitive security operations in response to the macro security operation.

Blaker in analogous art, however, discloses a method of executing a plurality of primitive security operations at a second processor in response to the macro security operation, and to generate a set of data from the execution of the plurality of primitive security operations. (Page 2, paragraph 11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Bellwood to include a method of executing a plurality of primitive security operations at a second processor in response to the macro security operation call and to generate a set of data from the execution of the plurality of primitive security operations. This modification would have been obvious because a person having ordinary skill in the art would have

been motivated to do so, as suggested by, Blaker (Page 1, paragraph 4) in order to allow a host processor to download one or more command and instruct the co-processor to execute one or more of the downloaded commands.

Both references do not explicitly disclose a macro security operation associated with a plurality of primitive security operations.

Mauro in analogous art, however, discloses a macro instruction operation associated with a plurality of primitive security operations. (Page 2, paragraphs 27-28; Page 3, paragraph 29; during secure session, such as in SSL, ...when a primitive cryptographic function is required, the CPU downloads the DSP assembly image, downloadable executable instructions executed by the DSP, through the shared memory)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Bellwood and Blaker to include a macro instruction operation associated with a plurality of primitive security operations. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to accelerate the performance of complex encryption and authentication algorithms needed in implementing security protocols, such as SSL, IPSec and WAP with a minimum delay and a minimum cost. (Page 1, paragraphs 5-6, Mauro)

As per claim 13:

The combination of Blaker, Bellwood and Mauro teaches all the subject matter as discussed above. In addition, Bellwood further discloses a system wherein the first

network element to request the secure session comprises the first network element to transmit a set of messages to the second network element, (Col. 5, lines 30-31, Bellwood) to execute a second macro security operation, and to generate a second set of data from the execution of the second macro security operation. (Col. 5, lines 41-53)

As per claim 14:

The combination of Blaker, Bellwood and Mauro teaches all the subject matter as discussed above. In addition, Bellwood further discloses a system comprising a third network element networked to the second network element, the third network element to request a second secure session with the second network element. (Col. 4, lines 65-67 and Col. 5, lines 1-2)

As per claim 15:

The combination of Blaker, Bellwood and Mauro teaches all the subject matter as discussed above. In addition, Bellwood further discloses a system comprising: the first network element to request a second secure session with the second network element; and the second network element to execute a second macro security operation to establish the second secure session with the first network element. (Col. 2, lines 49-50)

6. Claims 16-18, 20-22 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blaker (hereinafter Blaker) United States Publication Number 2002/0004904 in view of Mauro et al. (hereinafter Mauro) Unites States Publication Number 2002/0146128.

As per claims 16 and 21:

Blaker teaches an apparatus comprising:

a first processor to call a macro security operation to establish a secure session; (Page2, paragraph 11)

a second processor coupled to the first processor, the second processor to perform a plurality of primitive security operations in response to the macro security operation call; (Page 2, paragraph 11) and

a memory coupled to the first and the second processor, the memory to store a set of data generated by the second processor. (Figure 1, 36 and 22; Page 2, paragraph 11; Page 3, paragraph 34)

Blaker does not explicitly disclose a macro security operation associated with a plurality of primitive security operations to establish secure session.

Mauro in analogous art, however, discloses a macro instruction operation associated with a plurality of primitive security operations to establish secure session. (Page 2, paragraphs 27-28; Page 3, paragraph 29; during secure session, such as in SSL, ...when a primitive cryptographic function is required, the CPU downloads the DSP assembly image, downloadable executable instructions executed by the DSP, through the shared memory)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker to include a macro instruction operation associated with a plurality of primitive security operations to establish secure session. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to accelerate the performance of complex encryption and authentication algorithms

needed in implementing security protocols, such as SSL, IPSec and WAP with a minimum delay and a minimum cost. (Page 1, paragraphs 5-6, Mauro)

As per claim 17:

The combination of Blaker and Mauro teaches all the subject matter as discussed above. In addition, Blaker further discloses an apparatus wherein the second processor comprises: a request unit to fetch and to distribute the macro security operation; (Page 3, paragraph 34) and a plurality of execution units coupled to the request unit, one of the plurality of execution units to execute the plurality of primitive security operations. (Page 3, paragraph 34)

As per claims 18 and 24:

The combination of Blaker and Mauro teaches all the subject matter as discussed above. In addition, Blaker further discloses an apparatus wherein comprising: the first processor to call a second macro security operation after calling the first macro security operation; (Page 3, paragraph 39) and a second one of the plurality of execution units to execute a second plurality of primitive security operations corresponding to the second macro security operation before the one of the plurality of execution units completes execution of the plurality of primitive security operations. (Page 3, paragraph 39)

As per claims 20 and 22:

The combination of Blaker and Mauro teaches all the subject matter as discussed above. In addition, Blaker further discloses an apparatus further comprising the memory to store a set of source data. (Figure 1, 36 and 22)

7. Claims 19 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blaker (hereinafter Blaker) United States Publication Number 2002/0004904 in view of Mauro et al. (hereinafter Mauro) Unites States Publication Number 2002/0146128 and further in view of Tremblay et al. (hereinafter Tremblay) United States Letter Patent Number 5,925,123.

As per claim 19 and 23:

The combination of Blaker and Mauro teaches all the subject matter as discussed above. In addition, Blaker further discloses an apparatus wherein: an execution queue unit coupled to the microcode unit, the execution queue unit to queue the plurality of primitive security operations; (Figure 1, 44 and 46; Page 3, paragraph 34) a plurality of primitive security operation units coupled to the execution queue unit, the plurality of primitive security operation units to perform the plurality of primitive security operations; (Page 3, paragraph 39) and a bus coupled to the plurality of primitive security operation units, the bus to transmit data. (Figure 1, 24; Page 3, paragraph 33)

Both references do not explicitly disclose an apparatus comprising a microcode unit to translate the macro security operation into a plurality of primitive security operations.

Tremblay in analogous art, however, discloses an apparatus wherein the one of the plurality of execution units comprises: a microcode unit to translate the macro security operation into a plurality of primitive security operations. (Col. 3, lines 21-27)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker and Mauro to include a microcode unit to translate the macro security operation into a plurality of primitive security operations. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Tremblay (Abstract) in order to provide a dual instruction set processor that is capable of executing instruction in two different instructions sets from two different sources.

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay SG
2/24/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER